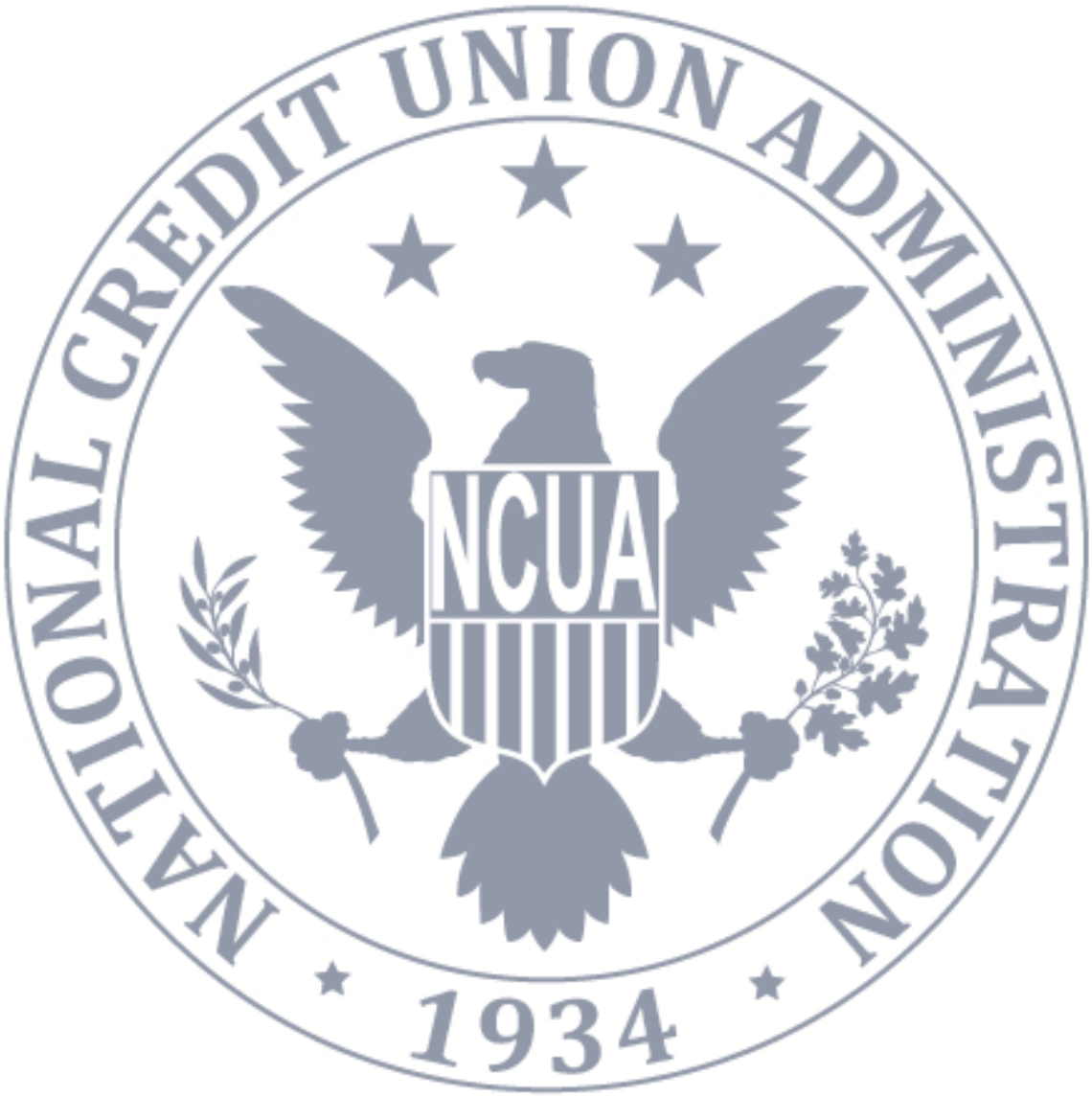
NCUA
National Credit Union Administration

Privacy Impact Assessment for Credit Union Service Organization Registry

Fiscal Year 2021

[This page intentionally left blank]



About this Document

A Privacy Impact Assessment (PIA) is an analysis of how PII is handled to ensure that handling conforms to applicable privacy requirements, to determine the privacy risks associated with an information system or activity, and to evaluate ways to mitigate privacy risks. A PIA is both an analysis and a formal document detailing the process and the outcome of the analysis.

Program offices and system owners are required to complete a PIA whenever they develop, procure, or use information technology to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII.[1] Completion of a PIA is a precondition for the issuance of an authorization to operate.[2]

Basic Information about the System

System Name: Credit Union Service Organization Registry CUSO Registry

NCUA Office of Primary Interest: Office of Examination and Insurance

Threshold		
1	*What is the status of the system/tool/application (for simplicity referred to as "system" going forward)?*	Operational
2	*Describe the system in 1-2 sentences.*	The CUSO Registry system is a publicly available application to support the registration of CUSOs. The purpose of gathering CUSO data is to increase consistency and transparency of CUSO information and address any potential systemic safety and soundness concerns stemming from relationships between credit unions and CUSOs.

[1] 44 U.S.C. § 3501, note; Pub. L. 107–347, § 208(b).
[2] OMB Memorandum M-14-04, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Act and Agency Privacy Management* (2013).

Purpose and Authority

The NCUA should only create, collect, use, process, store, maintain, disseminate, or disclose PII if it has authority to do so, and such authority should be identified in the appropriate notice.

The NCUA should provide notice of the specific purpose for which PII is collected and should only use, process, store, maintain, disseminate, or disclose PII for a purpose that is explained in the notice and is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.

Purpose and Authority		
1	*What is the purpose of the system?*	The purpose of gathering CUSO data is to increase consistency and transparency of CUSO information and address any potential systemic safety and soundness concerns stemming from relationships between credit unions and CUSOs.
2	*How is the PII collected/maintained/used in the system relevant and necessary to achieve the purpose described above?*	The PII is necessary in order to create the user accounts for CUSO contacts, CUSO Chief Executive Officers (CEOs), CUSO owners and all individuals who establish CUSO Registry System online accounts. The system collects e-mail addresses for purposes of user account verification and management.
3	*What is the legal authority to collect, maintain, use, or share the PII contained in the system?*	12 U.S.C. 1756, 1757(5)(D) and (7)(I), 1766, 1781(b)(9), 1782, 1784, 1785, 1786 and 1789(11).; 12 CFR parts 712 and 741.

Minimization

The NCUA should only create, collect, use, process, store, maintain, disseminate, or disclose PII that is directly relevant and necessary to accomplish a legally authorized purpose, and should only maintain PII for as long as is necessary to accomplish that purpose.

The NCUA recognizes the increased sensitivity of Social Security numbers (SSNs) and therefore makes every effort to limit the collection and maintenance of them. The NCUA also limits its collection of other types of PII to those that are necessary.

SSNs		
1	*Will the system collect, maintain, or share social security numbers?*	• No

PII		
1	*Basic Demographic*	• Email Address • Fax Number • First Name • Last Name • Middle Name (or initial) • Phone Number
1.1	*Who is it collected for?*	• Others: CUSOs users/officers/owners
2	*Medical and Family*	• None
3	*Financial*	• Other: Financial information regarding the CUSO business, not the individuals
4	*Biometric*	• None
5	*Employment and Education*	• None
6	*Information Technology (IT)*	• Login/Activity Records • Password • Username
6.1	*Who is this information collected for?*	• NCUA Employees/Contractors • Others: CUSO users/officers/owners; SSA users
7	*NCUA Employment*	• NCUA Email Address • Other: Active directory username; role-based security group
7.1	*Who is this information collected for?*	• NCUA Employees/Contractors • Others: SSA users

Collection and Consent

The NCUA should create, collect, use, process, store, maintain, disseminate, or disclose PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.

The NCUA should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. The NCUA should also establish procedures to receive and address individuals' privacy-related complaints and inquiries.

The NCUA endeavors both to collect information from the subject individual, and to attain affirmative informed consent, whenever possible. The NCUA's use of Privacy Act statements and privacy notices on forms are critical to this effort. For more information see the Transparency section below.

Collection and Consent		
1	*What are the sources from which the PII will be collected?*	• Within NCUA • The individual the information is about • Other SSAs
2	*How will the information be collected?*	• Web-based Form or Email
3	*Will the individuals whose information is collected/maintained in the system consent to their personal information?*	• Not specifically, but the individuals consented to providing the information originally and likely anticipated that their information would also be maintained and used this way.
4	*Will individuals be able to "opt-out" by declining to provide PII or by consenting only to a particular use?*	• No

Procedures to Address Individuals' Privacy Related Complaints and Inquiries

The Privacy team knows that complaints, concerns, and questions from individuals can be a valuable source of input that improves operational models, uses of technology, data collection practices, and privacy safeguards. To facilitate this type of feedback, the Privacy team has established the Privacy Complaint Process to receive and respond to

complaints, concerns, and questions from individuals about the NCUA's privacy practices. The process is described on the NCUA's privacy website. The Privacy team appropriately records and tracks complaints, concerns, and questions to ensure prompt remediation.

Maintenance and Use

The NCUA should establish administrative, technical, and physical safeguards to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.

The NCUA implements, documents, and tests security and privacy controls as required by applicable NIST and OMB guidance. Access controls are of particular importance with regard to protecting individuals' privacy. Records management, both keeping records for the required time frame and timely destroying or accessioning them, is also a key component of managing privacy risks.

Maintenance and Use		
1	*Which statement is most accurate?*	• NCUA owns the System.
2	*Who has access to PII in the system?*	• NCUA Employees • NCUA Contractors • Other: SSA employees; CUSO admin users have access to PII related to their specific CUSO
3	*Which roles have access to PII in the system?*	• Some System Users • System Administrators • Developers

Records Management		
1	*Which records retention schedule(s) will apply to this system?*	• Records Schedule Pending

Transparency

The NCUA should be transparent about information policies and practices with respect to PII, and should provide clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.

The NCUA's transparency efforts include providing adequate notice to individuals prior to collection of their PII. The NCUA achieves this with Privacy Act statements, or privacy notices (the latter if the collection is not associated with a Privacy Act System of Records), and compliance with the Paperwork Reduction Act.[3] The NCUA also publishes Systems of Records Notices in the Federal Register and makes them available on the privacy page of the NCUA's website.

Transparency			
1	*Will any forms or surveys be used to collect the information?*	• Yes	
	Title	*OMB No.*	*Privacy Act Statement or Privacy Notice?*
	CUSO User Registration Form	3133-0149	Privacy Act Statement

SORNs		
1	*Is the information in the system retrieved by a personal identifier?*	• Yes
2	*Applicable SORN*	NCUA-18

Accountability

The NCUA should be accountable for complying with these principles and applicable privacy requirements, and should appropriately monitor, audit, and document

[3] See the Collection and Consent section above.

compliance. The NCUA should also clearly define the roles and responsibilities with respect to PII for all employees and contractors, and should provide appropriate training to all employees and contractors who have access to PII.

Compliance with the Fair Information Privacy Principles

As evidenced by this PIA (and the other information publicly available on the privacy page of NCUA's website), the NCUA is committed to achieving and maintaining compliance with the Fair Information Privacy Principles.

Roles and Responsibilities of NCUA Staff

As detailed in the NCUA Acceptable Use Policy and applicable Rules of Behavior, all NCUA staff are responsible for protecting PII from unauthorized exposure and for reducing the volume and types of PII necessary for program functions. Staff must protect all PII that they handle, process, compile, maintain, store, transmit, or report on in their daily work.

To protect PII, staff must use proper collection, storage, transportation, transmission, and disposal methods, must not access PII beyond what they need to complete their job duties, and must not disclose PII to unauthorized parties. Managers are also responsible for providing their subordinates with context-specific practical guidance about protecting PII.

All NCUA staff are required to review and acknowledge receipt and acceptance of applicable Rules of Behavior upon gaining access to the NCUA's information systems and associated data.

Failure to protect PII may result in administrative sanctions, and criminal and/or civil penalties.[4]

Training

Together with the Office of Human Resources, the Privacy team ensures that new employees complete mandatory privacy training, and all existing employees and contractor employees complete privacy refresher training once every fiscal year. NCUA staff electronically certify acceptance of their privacy responsibilities as a part

[4] 5 U.S.C. § 552a(i)(3); NCUA Computer Security Rules of Behavior.

of annual privacy refresher training. The Privacy team keeps auditable records of completion of all mandatory trainings.

Analysis and Approval

This PIA was approved by or on behalf of the Senior Agency Official for Privacy. Below are additional details regarding the review and approval of the PIA.

Analysis and Approval	
Privacy Risk:	Acceptable
Approval Date:	July 20, 2021